Exhibit 6, Part 2

- Client A was a private company that had been incorporated in the British Virgin Islands on 3 June 2014. The sole director and shareholder of Client A was a Dubai based individual who had held a senior position at SCP. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.

- Client B was a private company that had been incorporated in the British Virgin Islands on 5 June 2014. The CV supplied for the director of Client B showed that he was a current employee of SCP. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.

- Client C was a private company incorporated in the Cayman Islands on 18 February 2013. The client's KYC documents showed that one of the two directors was 21 years old and had a total of four months experience working at a financial services firm that was subsequently purchased by the Solo Group on 6 July 2015. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.

- Client D was a private company that had been incorporated in the Cayman Islands on 4 October 2013. The sole director and shareholder was a Dubai based individual. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.

4.130 On 17 June 2014, Bastion received onboarding requests from a further three clients:

- Client E was a private company incorporated in the Seychelles on 28 April 2014. The sole director and shareholder was an individual who held a senior position at SCP until 2013.

- Client F was a private company incorporated in the Seychelles on 25 March 2014. The sole director and shareholder was a Hong Kong based individual who was a current employee of SCP.

- Ganymede was a private company incorporated in the Cayman Islands on 16 June 2010. The sole director and shareholder was Sanjay Shah.

4.131 Bastion stated that it felt pressured by SCP to urgently onboard these clients, particularly as it was told that one of the client entities was owned by Sanjay Shah. On the morning of 18 June 2014, Bastion confirmed to SCP that it had onboarded six of the entities but was yet to receive KYC documents for Client F.

SCP thanked Bastion for onboarding the entities so quickly and sent the remaining KYC documents to the Firm at 09:16 on 18 June 2014.

4.132 Three hours later, between 12:49 and 13:29, Bastion received a series of trade orders via email from Clients A to F requesting to buy equity shares in varying volumes in a German listed stock ("German stock A"). All of the orders requested an identical specific intraday purchase price of €160.1, which was around the same as the market closing price on 17 June 2014 of €160.12, but below the exchange price at 12:49 of €160.95. One of the orders from Client E was written as if the trade had already been agreed, which was also suggestive of the co-ordinated nature of the trades. It stated "*[Client E] buys [German stock A], 668,521 160.1*". This was subsequently corrected by the client, who re-sent the order in a "*more cleanly written*" format.

4.133 At 13:12, Bastion sought liquidity from Ganymede and stated "I have some form on [German stock A], are you in the market today for this?" A few minutes later another email from Bastion to Ganymede stated "I need to buy 3303496, can you show me an offer please?". At 13:47 Ganymede responded and stated that it could sell 3,964,905 shares at a price of €160.10. This in fact corresponded to the total number of shares in German stock A requested by Clients A to F and at the requested identical specific intraday purchase price of €160.1.

4.134 At 14:23, approximately an hour after the trades had been agreed, Ganymede indicated that it wanted to buy back the 3,964,905 shares in German stock A, equivalent to the amount it had just sold. Bastion approached Clients A to F who all replied agreeing to sell the shares they had just purchased. Five of the six clients proactively offered an identical price of €160.97, which was accepted by Ganymede. This price was €0.87 above the price Ganymede had sold the shares for, but was below the current exchange price of €161.05. At 15:10, Bastion confirmed to Ganymede that it had purchased all 3,964,905 German stock A shares at a price of €160.97.

4.135 The result of the trading was that Ganymede sold 3,964,905 shares in German stock A for consideration of €634,781,290.50 to six clients (Clients A to F). It then re-purchased the same shares an hour later at a higher price for consideration of €638,230,757.85, resulting in a net loss to Ganymede of €3,449,467.35, to the benefit of Clients A to F.

The timing of the orders was as follows:

Time of order	Buyer	Time of Trade	Seller	Quantity	Unit Price (€)	Consideration (€)
12:49:53	Client E	13:47	Ganymede	668,521	160.1	107,030,212.10
12:55:53	Client B	13:47	Ganymede	653,125	160.1	104,565,312.50
12:55:54	Client F	13:47	Ganymede	658,963	160.1	105,499,976.30
12:57:36	Client A	13:47	Ganymede	673,505	160.1	107,828,150.50
13:00:58	Client D	13:47	Ganymede	649,382	160.1	103,966,058.20
13:29:19	Client C	13:47	Ganymede	661,409	160.1	105,891,580.90
14:23	Ganymede	14:36	Client D	649,382	160.97	104,531,020.54
14:23	Ganymede	14:36	Client A	673,505	160.97	108,414,099.85
14:23	Ganymede	14:38	Client E	668,521	160.97	107,611,825.37
14:23	Ganymede	14:42	Client B	653,125	160.97	105,133,531.25
14:23	Ganymede	14:52	Client F	658,963	160.97	106,073,274.11
14:23	Ganymede	15:05	Client C	661,409	160.97	106,467,006.73

4.136 Another possible indicator of the co-ordinated nature of these Ganymede trades was that at 16:16 Ganymede indicated to Bastion that it wanted to trade again and would be "*send*[ing] *something through shortly*". However, at 16:29, it was not Ganymede but Client E that sent through an order to buy German stock A at a specific price of €160.25. This was quickly followed by similar trade orders from Client F and Client A, which prompted Bastion to email Ganymede at 16:44 asking if it had any German stock A to sell. At 16:55, Ganymede replied offering to sell 11,279,140 shares (which was the exact cumulative total of the trade orders from Clients E, F and A to whom it had sold and then repurchased the shares from just ninety minutes earlier) at the same specific price of €160.25. At 16:58, Bastion confirmed to Ganymede that the order had been filled.

4.137 Just two minutes later, Ganymede began the process of unwinding the trade and buying back the shares at a higher price, as it had done earlier that day. This time, the price Ganymede specified was €161.25, which was €1 more per share

than it had sold them for, and above the market closing price of €161. After receiving the order from Ganymede, Bastion approached Clients A, E and F and re-purchased the shares, resulting in a loss of €11,279,140 for Ganymede.

The timing of the orders was as follows:

Time of order	Buyer	Time of Trade	Seller	Quantity	Unit Price (€)	Consideration (€)
16:29	Client E	16:58	Ganymede	4,657,387	160.25	746,346,266.75
16:31	Client F	16:58	Ganymede	4,107,702	160.25	658,259,245.50
16:39	Client A	16:58	Ganymede	2,514,051	160.25	402,876,672.75
17:00	Ganymede	17:07	Client A	2,514,051	161.25	405,390,723.75
17:00	Ganymede	17:13	Client F	4,107,702	161.25	662,366,947.50
17:00	Ganymede	17:17	Client E	4,657,387	161.25	751,003,653.75

4.138 The methodology described above was again employed by Ganymede and other Solo Clients linked to the Solo Group in a series of trades executed by Bastion on 19 June 2014, 30 June 2014 and 20 May 2015, resulting in a total loss to Ganymede of €22,729,508.15 across the four days.

Analysis of the Ganymede *Trades*

4.139 All of the Ganymede trades involved the shares purportedly being repurchased by Ganymede the same day, within the T+2 or T+3 settlement period, and therefore the shares did not need to be transferred. The net result of the trading was that a total of €22,729,508.15 was owed by Ganymede to the other clients.

4.140 Bastion has confirmed that it was aware that the Ganymede trades resulted in losses to Ganymede. However, it failed to question the rationale for the trading as it considered that there might have been other simultaneous transactions involving the same clients, that the Firm was not privy to. However, Bastion was the only broker involved in these trades and in each instance arranged the buy and sell transactions. Even if there had been other legs of the transactions that

Bastion was not aware of, Bastion ought to have recognised from the buy and sell transactions that the losses to Ganymede resulted in direct profits for the other counterparties. At a minimum, this should have caused the Firm to question the clients about the rationale for the trading and consider whether the nature of these series of transactions were suspicious.

4.141 Furthermore, if Bastion had examined the trade orders prior to trading on 18 June 2014, or for the purpose of transaction monitoring and post trade surveillance after trading, it ought to have noticed that the requested volume of 11,279,140 shares on 18 June 2014 was 17 times the Average Daily Volume (ADV) of German stock A shares sold on European exchanges. If Bastion had noticed this red flag on receiving the trade order, it should have declined to execute the trade, or at a minimum queried the volumes with the clients.

4.142 Instead, Bastion failed to identify and/or flag any queries in relation to the unusual features of the Ganymede trades, either internally, or with the clients, or the Solo Group, including:

a) why the clients had to be urgently onboarded;

b) why the majority of the clients' directors/UBOs were connected to the Solo Group;

c) why the shares were purchased and sold at intraday prices, instead of the usual end of day price;

d) why the trades were unwound on the same day;

e) why the orders from clients A, B, D, E and F specified identical prices;

f) why the specified price was below the current intraday market price;

g) why the volume of shares transacted was 17 times the ADV of German Stock A shares sold on European exchanges;

h) why Ganymede would want to buy back the shares it had sold a short while earlier at a higher price, resulting in a loss for it on each occasion; and

i) why the Ganymede trades on 20 May 2015 took place by email, even though all other Solo Trading took place on Brokermesh at that time;

4.143 At a minimum, these red flags should have prompted Bastion to question the clients about the purpose of the trading, however Bastion did not query the

Ganymede trades with Ganymede or flag the potential loss to the client before or after execution.

4.144 Bastion ought to have queried how these clients would have been able to source such sizeable liquidity in such short order, whether this liquidity was in line with the trading levels which could be expected from these clients, given the information previously obtained through CDD.

4.145 Bastion has stated that it did not have any suspicions about the Ganymede trades as it trusted Sanjay Shah's reputation. This raises serious concerns about the firm's risk appetite and the extent and effectiveness of its transaction monitoring.

End of the Purported Solo Trading

4.146 Bastion executed its last trade for a Solo Client on 29 September 2015. The Solo Clients ceased the purported trading with all the six Broker Firms after unannounced visits by the Authority to the offices of the Solo Group entities and the Broker Firms between 2 – 4 November 2015.

Bastion failed to Identify Any of the Above Issues

4.147 Bastion failed to identify any of the above issues. With respect to AML, in both 2014 and 2015, Bastion did not identify any transactions raising any suspicions and no breaches were reported or observed.

5. FAILINGS

5.1 The statutory and regulatory provisions relevant to this Notice are referred to in Annex B.

5.2 The JMLSG Guidance has also been included in Annex B, because in determining whether breaches of its rules on systems and controls against money laundering have occurred, and in determining whether to take action for a financial penalty or censure in respect of a breach of those rules, the Authority has also had regard to whether Bastion followed the JMLSG Guidance.

Principle 3

5.3 Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

5.4 Bastion breached this requirement during the Relevant Period, in relation to business related to the Solo Group, as its policies and procedures were inadequate for identifying, assessing and mitigating the risk of financial crime as they failed to:

5.4.1 Establish the requirement for risk assessments to be documented, as well as to document the rationale for any due diligence measures the firm waived when compared to its standard approach, in view of its risk assessment of a particular customer;

5.4.2 Set out adequate processes and procedures for EDD;

5.4.3 Set out adequate processes and procedures for client categorisation;

5.4.4 Set out adequate processes and procedures for transaction monitoring, including how transactions are monitored, and with what frequency, and set out adequate processes and procedures for how to identify suspicious transactions.

Principle 2

5.5 The Authority considers that Bastion failed to act with due skill, care and diligence as required by Principle 2 to properly assess, monitor and manage the risk of financial crime associated with the business related to the Solo Group in that the Firm:

a) Failed to properly conduct customer due diligence prior to onboarding, and consequently failed to identify that the Solo Clients presented a higher risk of financial crime before they started trading;

b) Failed to gather adequate information to enable it to understand the purpose and intended nature of the business that the Solo Clients were going to undertake, the likely size or frequency of the purported trading intended by the Solo Clients or their source of funds;

c) Failed to undertake and document a risk assessment for each of the Solo Clients prior to onboarding and trading for the Solo Clients;

d) Failed to complete EDD for any of the Solo Clients despite the fact that none of the Solo Clients were physically present for identification purposes and a number of other risk factors were present;

e) Failed to assess each of the Solo Clients against the categorisation criteria set out in COBS 3.5.2R and failed to record the results of such assessments, including sufficient information to support the categorisation, contrary to COBS 3.8.2(2)(a);

f) Failed to conduct transaction monitoring of the Solo Clients' purported trades;

g) Failed to recognise numerous red flags with the purported trading, including failing to consider whether it was plausible and/or realistic that sufficient liquidity was sourced within a closed network of entities for the size and volumes of trading conducted by the Solo Clients. Likewise, failing to consider or recognise that the profiles of the Solo Clients meant that they were highly unlikely to meet the scale and volume of the trading purportedly being carried out, and/or failed to at least obtain sufficient evidence of the clients' source of funds to satisfy itself to the contrary; and

h) Failed to recognise numerous red flags arising from the purported Ganymede trades and adequately consider financial crime and money laundering risks they posed to the Firm.

6. SANCTION

6.1 The Authority has considered the disciplinary and other options available to it and has concluded that a financial penalty is the appropriate sanction in the circumstances of this particular case.

6.2 The Authority's policy on the imposition of financial penalties is set out in Chapter 6 of DEPP. In determining the proposed financial penalty, the Authority has had regard to this guidance.

6.3 DEPP 6.5A sets out a five-step framework to determine the appropriate level of financial penalty.

Step 1: disgorgement

6.4 Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify.

6.5 The financial benefit associated with Bastion's failings is quantifiable by reference to the revenue it derived from the business related to the Solo Group as described in the Notice.

6.6 The figure after Step 1 is therefore **£1,554,855.40**.

Step 2: the seriousness of the breach

6.7 Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.8 The Authority considers that the revenue generated by Bastion is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of Bastion's revenue during the period of the breach.

6.9 Bastion's revenue is the revenue derived from business associated with the Solo Group. The period of Bastion's breach was between 29 January 2014 and 29 September 2015. The Authority considers Bastion's revenue for this period to be £1,554,855.40.

6.10 In deciding on the percentage of the revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach; the more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels:

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

6.11 In assessing the seriousness level, Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. DEPP 6.5A.2G lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:

1. The breaches revealed serious or systemic weaknesses in both the Firm's procedures and the management systems or internal controls relating to all or part of the Firm's business; and

2. The breaches created a significant risk that financial crime would be facilitated, occasioned or otherwise occur.

6.12 Taking all of these factors into account, Authority considers the seriousness of the breach to be level 4 and so the Step 2 figure is 15% of £1,554,855.40.

6.13 Step 2 is therefore **£233,228.31.**

Step 3: Mitigating and aggravating factors

6.14 Pursuant to DEPP 6.5A.3G, at Step 3, the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

6.15 The Authority considers that the following factors aggravates the breach:

(1) The Authority and the JMLSG have published numerous documents highlighting financial crime risks and the standards expected of firms when dealing with those risks. The most significant publications include the JMLSG Guidance and Financial Crime Guide (including the thematic reviews that are referred to therein) which was first published in December 2011. These publications set out good practice examples to assist firms, for example in managing and mitigating money laundering risk by (amongst other things) conducting appropriate customer due diligence, monitoring of customers' activity and guidance of dealing with higher-risk situations. Given the number and detailed nature of such publications, and past enforcement action taken by the Authority in respect of similar failings by other firms, Bastion should have been aware of the importance of appropriately assessing, managing and monitoring the risk that the Firm could be used for the purposes of financial crime.

6.16 Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 10%.

6.17 Step 3 is therefore **£256,551.14.**

Step 4: adjustment for deterrence

6.18 Pursuant to DEPP 6.5A.4G, if the Authority considers that the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further of similar breaches, then the Authority may increase the penalty.

6.19 The Authority considers that DEPP 6.5A.4G(1)(a) is relevant in this instance and has therefore determined that this is an appropriate case where an adjustment for deterrence is necessary. Without an adjustment for deterrence, the financial penalty would be £256,551.14. In the circumstances of this case, the Authority considers that a penalty of this size would not serve as a credible deterrent to Bastion and others. This small penalty does not meet the Authority's objective of credible deterrence. As a result, it is necessary for the Authority to increase the penalty to achieve credible deterrence.

6.20 Having taken into account the factor outlined in DEPP 6.5A.4G, the Authority considers that a multiplier of five should be applied at Step 4.

6.21 Step 4 is therefore **£1,282,755.71.**

Step 5: settlement discount

6.22 Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement. The settlement discount does not apply to the disgorgement of any benefit calculated at Step 1.

6.23 The Authority and Bastion did reach agreement to settle so a 30% discount applies to the Step 4 figure.

6.24 The total financial penalty (that would have been imposed) is therefore **£2,452,700**.

7. PROCEDURAL MATTERS

7.1 This Notice is given to Bastion under and in accordance with section 390 of the Act.

7.2 The following statutory rights are important.

Decision maker

7.3 The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

Manner and time for payment

7.4 The financial penalty must be admitted in the liquidation of the Firm by no later than 14 days from the date of the Final Notice. The financial penalty will be ranked with other creditors of the Firm but the Authority will keep it under review in order that legitimate creditors are satisfied prior to any funds realised in the liquidation being used to pay some, or all, of the financial penalty.

Publicity

7.5 Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

7.6 The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

Authority contacts

7.7 For more information concerning this matter generally, contact Giles Harry (direct line: 020 7066 8072) at the Authority.

Mario Theodosiou

Head of Department

Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A: CHRONOLOGY

2004	Bastion was incorporated and authorised by the Authority.
January 2014	Initial discussions took place with SCP.
19 February 2014	Bastion signed a custody agreement with SCP.
29 January-April 2014	Initial onboarding of Solo Clients.
26 February 2014	Trading commenced in Danish stocks.
17 April 2014	Trading commenced in Belgian stocks.
16/17 June 2014	"Urgent" onboarding of 7 new clients.
18/19/30 June 2014	Trades in German and Belgian stocks via the 7 recently onboarded clients, resulting in total losses to Ganymede Cayman of €18.52 million.
27 January 2015	Further services agreement with Solo Group signed by Bastion.
28 January 2015	Services Agreements and Transaction Reporting Notices signed with West Point and Telesto.
3 February 2015	Services Agreement signed with OPL.
18 February 2015	Brokermesh licence agreement signed.
25 February 2015	Trading on Brokermesh commenced.
20 May 2015	Further trade in German stock resulting in a loss of €1.86m for Ganymede Cayman.
1 June 2015	Last cum-dividend trade in Belgian stock by Bastion on Brokermesh.
6 August 2015	Last batch of Solo Clients onboarded by Bastion.
7 August 2015	Last cum-dividend trade in Danish stock by Bastion on Brokermesh
29 September 2015	Last instance of Unwind Trading by Bastion for Solo Clients.
3 November 2015	Unannounced visit by the Authority.

ANNEX B: RELEVANT STATUTORY AND REGULATORY PROVISIONS

RELEVANT STATUTORY PROVISIONS

1.1 Pursuant to sections 1B and 1D of the Act, one of the Authority's operational objectives is protecting and enhancing the integrity of the UK financial system.

1.2 Pursuant to section 206 of the Act, if the Authority considers that an authorised person has contravened a requirement imposed on it by or under the Act, it may impose on that person a penalty in respect of the contravention of such amount as it considers appropriate.

THE 2007 REGULATIONS

1.3 Regulation 5 provides:

Meaning of customer due diligence measures

"Customer due diligence measures" means—

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and

(c) obtaining information on the purpose and intended nature of the business relationship."

1.4 Regulation 6 provides:

Meaning of beneficial owner

In the case of a body corporate, "beneficial owner" means any individual who—

(a) as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or

(b) as respects any body corporate, otherwise exercises control over the management of the body.

In the case of a trust, "beneficial owner" means—

(a) any individual who is entitled to a specified interest in at least 25% of the capital of the trust property;

(b) as respects any trust other than one which is set up or operates entirely for the benefit of individuals falling within sub-paragraph (a), the class of persons in whose main interest the trust is set up or operates;

(c) any individual who has control over the trust.

1.5 Regulation 7 provides:

Application of customer due diligence measures

(1) …, a relevant person must apply customer due diligence measures when he—

(a) establishes a business relationship;

(b) carries out an occasional transaction;

(c) suspects money laundering or terrorist financing;

(d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.

1.6 Regulation 8 provides:

Ongoing monitoring

"(1) A relevant person must conduct ongoing monitoring of a business relationship.

(2) "Ongoing monitoring" of a business relationship means—

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

(3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures. "

1.7 Regulation 14 provides:

Enhanced customer due diligence and ongoing monitoring

"(1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring—

(a) in accordance with paragraphs (2) to (4);

(b) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures—

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution."

1.8 Regulation 17 provides:

Reliance

"(1) A relevant person may rely on a person who falls within paragraph (2) (or who the relevant person has reasonable grounds to believe falls within paragraph (2)) to apply any customer due diligence measures provided that—

(a) the other person consents to being relied on; and

(b) notwithstanding the relevant person's reliance on the other person, the relevant person remains liable for any failure to apply such measures.

(2) The persons are—

(a) a credit or financial institution which is an authorised person;

…

(4) Nothing in this regulation prevents a relevant person applying customer due diligence measures by means of an outsourcing service provider or agent provided that the relevant person remains liable for any failure to apply such ***measures."***

1.9 Regulation 20 provides:

Policies and Procedures

"(1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to—

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) record-keeping;

(d) internal control;

(e) risk assessment and management;

(f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures,

in order to prevent activities related to money laundering and terrorist financing.

(2) The policies and procedures referred to in paragraph (1) include policies and procedures—

(a) which provide for the identification and scrutiny of—

(i) complex or unusually large transactions;

(ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;"

RELEVANT REGULATORY PROVISIONS

2.1 In exercising its powers to impose a financial penalty, the Authority has had regard to the relevant regulatory provisions published in the Authority's Handbook. The main provisions that the Authority considers relevant are set out below.

Principles for Business ("Principles")

2.2 The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook.

2.3 Principle 2 provides:

"A firm must conduct its business with due skill, care and diligence.

2.4 Principle 3 provides:

"A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

SENIOR MANAGEMENT ARRANGEMENTS, SYSTEMS AND CONTROLS ("SYSC")

2.5 SYSC 3.2.4G provides:

"The *guidance relevant to delegation within the firm is also relevant to external delegation ('outsourcing'). A firm cannot contract out its regulatory obligations. So, for example, under Principle 3 a firm should take reasonable care to supervise the discharge of outsourced functions by its contractor.*

A firm should take steps to obtain sufficient information from its contractor to enable it to assess the impact of outsourcing on its systems and controls."

2.6 SYSC 3.2.6E provides:

"The FCA, when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the guidance for the UK financial sector issued by the Joint Money Laundering Steering Group".

2.7 SYSC 3.2.6R provides:

"A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime."

2.8 SYSC 6.1.1R provides:

"A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime."

2.9 SYSC 6.3.1R provides:

A firm must ensure the policies and procedures established under SYSC 6.1.1 R include systems and controls that:

(1) enable it to identify, assess, monitor and manage money laundering risk; and

(2) are comprehensive and proportionate to the nature, scale and complexity of its activities.

2.10 SYSC 6.3.2G provides:

"Money laundering risk" is the risk that a firm may be used to further money laundering. Failure by a firm to manage this risk effectively will increase the risk to society of crime and terrorism.

2.11 SYSC 6.3.6 provides:

"In identifying its money laundering risk and in establishing the nature of these systems and controls, a firm should consider a range of factors, including:

(1) its customer, product and activity profiles;

(2) its distribution channels;

(3) the complexity and volume of its transactions;

(4) its processes and systems; and

(5) its operating environment".

2.12 SYSC 6.3.7 provides:

"A firm should ensure that the systems and controls include:

(3) appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies;

(4) appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:

(a) the development of new products;

(b) the taking-on of new customers; and

(c) changes in its business profile".

2.13 SYSC 9.1.1 R provides:

"A firm must arrange for orderly records to be kept of its business and internal organisation, including all services and transactions undertaken by it, which must be sufficient to enable the appropriate regulator or any other relevant competent authority under MiFID or the UCITS Directive to monitor the firm's compliance with the requirements under the regulatory system, and in particular to ascertain that the firm has complied with all obligations with respect to clients."

CONDUCT OF BUSINESS SOURCEBOOK (COBS)

2.14 COBS 3.3.1A(EU) provides:

"*Articles 45(1) and (2) of the MiFID Org Regulation require firms to provide clients with specified information concerning client categorisation.*

45(1) Investment firms shall notify new clients, and existing clients that the investment firm has newly categorised as required by Directive 2014/65/EU, of their categorisation as a retail client, a professional client or eligible counterparty in accordance with that Directive.

(2) Investment firms shall inform clients in a durable medium about any right that client has to request a different categorisation and about any limitations to the level of client protection that a different categorisation would entail.

[Note: articles 45(1) and (2) of the MiFID Org Regulation]"

2.15 COBS 3.3.1B(R) provides:

"*The information referred to in article 45(2) of the MiFID Org Regulation (as reproduced at COBS 3.3.1AEU) must be provided to clients prior to any provision of services.*

[*Note: paragraph 2 of section I of annex II to MiFID]*"

2.16 COBS 3.5.2 provides:

Per Se Professional Clients

"Each of the following is a per se professional client unless and to the extent it is an eligible counterparty or is given a different categorisation under this chapter:

(1) an entity required to be authorised or regulated to operate in the financial markets. The following list includes all authorised entities carrying out the characteristic activities of the entities mentioned, whether authorised by an EEA State or a third country and whether or not authorised by reference to a directive:

(a) a credit institution;

(b) an investment firm;

(c) any other authorised or regulated financial institution;

(d) an insurance company;

(e) a collective investment scheme or the management company of such a scheme;

(f) a pension fund or the management company of a pension fund;

(g) a commodity or commodity derivatives dealer;

(h) a local;

(i) any other institutional investor;

(2) in relation to MiFID or equivalent third country business a large undertaking meeting two of the following size requirements on a company basis:

(a) balance sheet total of EUR 20,000,000;

(b) net turnover of EUR 40,000,000;

(c) own funds of EUR 2,000,000;

(3) in relation to business that is not MiFID or equivalent third country business a large undertaking meeting any1of the following conditions:

(a) a body corporate (including a limited liability partnership) which has (or any of whose holding companies or subsidiaries has) (or has had at any time during the previous two years) 1called up share capital or net

assets 1of at least £51 million (or its equivalent in any other currency at the relevant time);

(b) an undertaking that meets (or any of whose holding companies or subsidiaries meets) two of the following tests:

(i) a balance sheet total of EUR 12,500,000;

(ii) a net turnover of EUR 25,000,000;

(iii) an average number of employees during the year of 250;

(c) a partnership or unincorporated association which has (or has had at any time during the previous two years) net assets of at least £5 million (or its equivalent in any other currency at the relevant time) and calculated in the case of a limited partnership without deducting loans owing to any of the partners;

(d) a trustee of a trust (other than an occupational pension scheme, SSAS, personal pension scheme or stakeholder pension scheme) which has (or has had at any time during the previous two years) assets of at least £10 million (or its equivalent in any other currency at the relevant time) calculated by aggregating the value of the cash and designated investments forming part of the trust's assets, but before deducting its liabilities;

(e) a trustee of an occupational pension scheme or SSAS, or a trustee or operator of a personal pension scheme or stakeholder pension scheme where the scheme has (or has had at any time during the previous two years):

(i) at least 50 members; and

(ii) assets under management of at least £10 million (or its equivalent in any other currency at the relevant time);

(f) a local authority or public authority.

(4) a national or regional government, a public body that manages public debt, a central bank, an international or supranational institution (such as the World Bank, the IMF, the ECP, the EIB) or another similar international organisation;

(5) another institutional investor whose main activity is to invest in financial instruments (in relation to the firm's MiFID or equivalent third country business) or designated investments (in relation to the firm's other business). This includes entities dedicated to the securitisation of assets or other financing transactions."

2.17 COBS 3.5.3 provides:

Elective professional clients

A firm may treat a client other than a local public authority or municipality3 as an elective professional client if it complies with (1) and (3) and, where applicable, (2):

(1) the firm undertakes an adequate assessment of the expertise, experience and knowledge of the client that gives reasonable assurance, in light of the nature of the transactions or services envisaged, that the client is capable of making his own investment decisions and understanding the risks involved (the "qualitative test");

(2) in relation to MiFID or equivalent third country business in the course of that assessment, at least two of the following criteria are satisfied:

(a) the client has carried out transactions, in significant size, on the relevant market at an average frequency of 10 per quarter over the previous four quarters;

(b) the size of the client's financial instrument portfolio, defined as including cash deposits and financial instruments, exceeds EUR 500,000;

(c) the client works or has worked in the financial sector for at least one year in a professional position, which requires knowledge of the transactions or services envisaged; (the "quantitative test"); and

(3) the following procedure is followed:

(a) the client must state in writing to the firm that it wishes to be treated as a professional client either generally or in respect of a particular service or transaction or type of transaction or product;

(b) the firm must give the client a clear written warning of the protections and investor compensation rights the client may lose; and

(c) the client must state in writing, in a separate document from the contract, that it is aware of the consequences of losing such protections.

2.18 COBS 3.8.2R provides:

(2) A firm must make a record in relation to each client of:

(a) the categorisation established for the client under this chapter, including sufficient information to support that categorisation;

…

DECISION PROCEDURE AND PENALTIES MANUAL ("DEPP")

2.19 Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act. In particular, DEPP 6.5A sets out the five steps for penalties imposed on firms.

ENFORCEMENT GUIDE

2.20 The Enforcement Guide sets out the Authority's approach to taking disciplinary action. The Authority's approach to financial penalties and suspensions (including restrictions) is set out in Chapter 7 of the Enforcement Guide.

JMLSG GUIDANCE– PART I (published 20 November 2013)

Outsourcing

3.16 Where AML/CTF tasks are delegated by a firm's MLRO, the FCA will expect the MLRO to take ultimate managerial responsibility.

Risk-based approach

4.14 A risk-based approach starts with the identification and assessment of the risk that has to be managed. Examples of the risks in particular industry sectors are set out in the sectoral guidance in Part II, and at www.jmlsg.org.uk.

4.8 A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the firm. These steps are to:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the firm's particular
  - customers and any underlying beneficial owners*;
  - products;
  - delivery channels;
  - geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks, in the context of the firm's risk appetite;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

* In this Chapter, references to 'customer' should be taken to include beneficial owner, where appropriate.

4.9 Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know at the outset of the relationship who their customers are, what they do, their expected level of activity with the firm and whether or not they are likely to be engaged in criminal activity. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions or activity that may be suspicious.

4.12 A risk assessment will often result in a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional customer information and monitoring for each category, in a way that minimises complexity.

4.15 While a risk assessment should always be performed at the inception of the customer relationship (although see paragraph 4.16 below), for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making the monitoring of transactions and on-going reviews a fundamental component of a reasonably designed RBA. A firm may also have to adjust its risk assessment of a particular customer based on information received from a competent authority.

4.34 Based on the risk assessment carried out, a firm will determine the level of CDD that should be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customer, based on the firm's risk appetite.

4.39 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. Guidance on the types of additional information that may be sought is set out in section 5.5.

4.40 Where the risks of ML/TF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious. Examples of EDD measures that could be applied for higher risk business relationships include:

- Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner
- Obtaining additional information on the intended nature of the business relationship

- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

4.50 Firms must document their risk assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities.

4.52 In addition, on a case-by-case basis, firms should document the rationale for any additional due diligence measures it has undertaken (or any it has waived) compared to its standard approach, in view of its risk assessment of a particular customer.

Customer due diligence

5.1.5 The CDD measures that must be carried out involve: (a) identifying the customer, and verifying his identity (see paragraphs 5.3.2ff); (b) identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.3.8ff); and (c) obtaining information on the purpose and intended nature of the business relationship (see paragraphs 5.3.20ff).

5.2.6 Where a firm is unable to apply CDD measures in relation to a customer, the firm (a) must not carry out a transaction with or for the customer through a bank account; (b) must not establish a business relationship or carry out an occasional transaction with the customer; (c) must terminate any existing business relationship with the customer; (d) must consider whether it ought to be making a report to the NCA, in accordance with its obligations under POCA and the Terrorism Act.

5.3.21 A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.

5.3.261 For situations presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money

laundering or terrorist financing risk. Also, some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering. In respect of trusts in the latter category, the firm's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Enhanced due diligence

5.5.1 A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship.

5.5.2 As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons: to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.

5.5.4 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.

5.5.5. A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

5.5.6 When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g., inheritance, divorce settlement, property sale), in order to decide whether to accept the application or continue with the relationship. The firm should consider whether, in some circumstances, evidence of source of wealth or

income should be required (for example, if from an inheritance, see a copy of the will). The firm should also consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

5.5.9 The ML Regulations prescribe three specific types of relationship in respect of which EDD measures must be applied. These are:

- where the customer has not been physically present for identification purposes (see paragraphs 5.5.10ff);
- in respect of a correspondent banking relationship (see Part II, sector 16: *Correspondent banking*);
- in respect of a business relationship or occasional transaction with a PEP (see paragraphs 5.5.18ff).

Reliance on third parties

5.6.4 The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is listed in Regulation 17(2), and that consent to being relied on has been given (see paragraph 5.6.8). The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.6.14 Whether a firm wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's regulated status, may include consideration of matters such as:

- its public disciplinary record, to the extent that this is available;
- the nature of the customer, the product/service sought and the
- sums involved;
- any adverse experience of the other firm's general efficiency in business dealings;
- any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the firm to be relied upon.

5.6.16 In practice, the firm relying on the confirmation of a third party needs to know:

- the identity of the customer or beneficial owner whose identity is being verified;
- the level of CDD that has been carried out; and
- confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information.

In order to standardise the process of firms confirming to one another that appropriate CDD measures have been carried out on customers, guidance

is given in paragraphs 5.6.30 to 5.6.33 below on the use of pro-forma confirmations containing the above information.

5.6.24 A firm must also document the steps taken to confirm that the firm relied upon satisfies the requirements in Regulation 17(2). This is particularly important where the firm relied upon is situated outside the EEA.

5.6.25 Part of the firm's AML/CTF policy statement should address the circumstances where reliance may be placed on other firms and how the firm will assess whether the other firm satisfies the definition of third party in Regulation 17(2) (see paragraph 5.6.6).

Monitoring customer activity

5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile;
- Ensuring that the documents, data or information held by the firm are kept up to date.

5.7.2 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

5.7.3 The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the right person(s); and
- appropriate action is taken on the findings of any further examination.

5.7.4 Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken

and in either case, unusual transactions or activities will be flagged for further examination.

5.7.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

5.7.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

JMLSG Part II – Wholesale Markets

Types of Risk

18.14 OTC and exchange-based trading can also present very different money laundering risk profiles. Exchanges that are regulated in equivalent jurisdictions, are transparent and have a central counterparty to clear trades, can largely be seen as carrying a lower generic money laundering risk. OTC business may, generally, be less well regulated and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products... Hence, when dealing in the OTC markets firms will need to take a more considered risk-based approach and undertake more detailed risk-based assessment.

JMLSG GUIDANCE– PART I (published 19 November 2014)

Risk-based approach

4.5 A risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the firm's philosophy, and as such reflected in the procedures and controls. There needs to be a clear communication of policies and procedures across the firm, along with the robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

4.6 Although the ML/TF risks facing the firm fundamentally arise through its customers, the nature of the business and their activities, it is important that the firm considers its customer risks in the context of the wider ML/TF environment inherent in the jurisdictions in which the firm and its customers operate. Firms should bear in mind that some jurisdictions have close links with other, perhaps higher risk jurisdictions, and where appropriate and relevant regard should be had to this.

4.9 The procedures, systems and controls designed to mitigate assessed ML/TF risks should be appropriate and proportionate to these risks, and should be designed to provide an effective level of mitigation.

4.12 A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks based by the firm. These steps are to:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the firm's particular
  - customers and any underlying beneficial owners*;
  - products;
  - delivery channels;
  - geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks, in the context of the firm's risk appetite;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

* *In this Chapter, references to 'customer' should be taken to include beneficial owner, where appropriate.*

4.13 Whatever approach is considered the most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know at the outset of the relationship who their customers are, where they operate, what they do, their expected level of activity with the firm and whether or not they are likely to be engaged in criminal activity. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions that may be suspicious.

4.20 In reaching an appropriate level of satisfaction as to whether the customer is acceptable, requesting more and more identification is not always the right answer – it is sometimes better to reach a full and documented understanding of what the customer does, and the transactions it is likely to undertake. Some business lines carry an inherently higher risk of being used for ML/TF purposes than others.

4.21 However, as stated in paragraph 5.2.6, if a firm cannot satisfy itself as to the identity of the customer; verify that identity; or obtain sufficient information on the nature and intended purpose of the business relationship, it must not enter into a new relationship and must terminate an existing one.

4.22 While a risk assessment should always be performed at the inception of a customer relationship (although see paragraph 4.16 below), for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making the monitoring of transactions and on-going reviews a fundamental component of a

reasonably designed RBA. A firm may also have to adjust its risk assessment of a particular customer based on information received from a competent authority.

4.25 For firms which operate internationally, or which have customers based or operating abroad, there are additional jurisdictional risk considerations relating to the position of the jurisdictions involved, and their reputation and standing as regards the inherent ML/TF risk, and the effectiveness of their AML/CTF enforcement regime.

4.45 Based on the risk assessment carried out, a firm will determine the level of CDD that should be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customer, based on the firm's risk appetite.

4.50 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. Guidance on the types of additional information that may be sought is set out in section 5.5.

4.51 Where the risks of ML/TF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious. Examples of EDD measures that could be applied for higher risk business relationships include:

- Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner
- Obtaining additional information on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards

4.61 Firms must document their risk assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities.

4.63 In addition, on a case-by-case basis, firms should document the rationale for any additional due diligence measures it has undertaken (or any it has waived) compared to its standard approach, in view of its risk assessment of a particular customer.

Customer due diligence

5.1.5 The CDD measures that must be carried out involve: (a) identifying the customer, and verifying his identity (see paragraphs 5.3.2ff); (b) identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.3.8ff); and (c) obtaining information on the purpose and intended nature of the business relationship (see paragraphs 5.3.20ff).

5.2.6 Where a firm is unable to apply CDD measures in relation to a customer, the firm (a) must not carry out a transaction with or for the customer through a bank account; (b) must not establish a business relationship or carry out an occasional transaction with the customer; (c) must terminate any existing business relationship with the customer; (d) must consider whether it ought to be making a report to the NCA, in accordance with its obligations under POCA and the Terrorism Act.

5.3.20 A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.

5.3.253 For situations presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering or terrorist financing risk. Also, some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering. In respect of trusts in the latter category, the firm's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Enhanced due diligence

5.5.1 A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner,

where applicable, and the purpose and intended nature of the business relationship.

5.5.2 As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons: to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.

5.5.4 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc. of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.

5.5.5 A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

5.5.6 When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending upon the nature of the product or service for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g., inheritance, divorce settlement, property sale), in order to decide whether to accept the application or continue with the relationship. The firm should consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

5.5.9 The ML Regulations prescribe three specific types of relationship in respect of which EDD must be applied. They are:

- where the customer has not been physically present for identification purposes (see paragraphs 5.5.10ff);
- in respect of a correspondent banking relationship (see Part II, sector 16: Correspondent banking);
- in respect of a business relationship or occasional transaction with a PEP (see paragraph 5.5.18ff).

Reliance on third parties

5.6.4 The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is

listed in Regulation 17(2), and that consent to be relied on has been given (see paragraph 5.6.8). The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.6.14 Whether a firm wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's regulated status, may include consideration of matters such as:

- its public disciplinary record, to the extent that this is available; the nature of the customer, the product/service sought and the sums involved; any adverse experience of the other firm's general efficiency in business dealings; any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the firm to be relied upon.

5.6.16 In practice, the firm relying on the confirmation of a third party needs to know:

- the identity of the customer or beneficial owner whose identity is being verified; the level of CDD that has been carried out; and confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information.

In order to standardise the process of firms confirming to one another that appropriate CDD measures have been carried out on customers, guidance is given in paragraphs 5.6.30 to 5.6.33 below on the use of pro-forma confirmations containing the above information.

5.6.24 A firm must also document the steps taken to confirm that the firm relied upon satisfies the requirements in Regulation 17(2). This is particularly important where the firm relied upon is situated outside the EEA.

5.6.25 Part of the firm's AML/CTF policy statement should address the circumstances where reliance may be placed on other firms and how the firm will assess whether the other firm satisfies the definition of third party in Regulation 17(2) (see paragraph 5.6.6).

Monitoring customer activity

5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile; Ensuring that the documents, data or information held by the firm are kept up to date.

5.7.2 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers,

assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

5.7.3 The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the right person(s); and
- appropriate action is taken on the findings of any further examination.

5.7.4 Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken

and in either case, unusual transactions or activities will be flagged for further examination.

5.7.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

5.7.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

JMLSG Part II – Wholesale Markets

Types of Risk

18.14 OTC and exchange-based trading can also present very different money laundering risk profiles. Exchanges that are regulated in equivalent jurisdictions, are transparent and have a central counterparty to clear trades, can largely be seen as carrying a lower generic money laundering risk. OTC business may, generally, be less well regulated and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products. For example, trades that are executed as OTC but then are centrally cleared, have a different risk profile to trades that are executed and settled OTC. Hence, when dealing in the OTC markets firms will need to take a more considered risk-based approach and undertake more detailed risk-based assessment.

ANNEX C - 401(k) Funds

Employer Created 401(k) Plans

A 401(k) is a qualified profit sharing plan that allows employees to contribute a portion of their wages to individual retirement accounts. Employers can also contribute to employees' accounts. Any money that is contributed to a 401(k) below the annual contribution limit is not subject to income tax in the year the money is earned, but then is taxable at retirement. For example, if John Doe earns $100,000 in 2018, he is allowed to contribute $18,500, which is the 2018 limit, to his 401(k) plan. If he contributes the full amount that he is allowed, then although he earned $100,000, his taxable income for income tax purposes would be $81,500. Then, he would pay income tax upon any money that he withdraws from his 401(k) at retirement. If he withdraws any money prior to age 59 1/2, he would be subject to various penalties and taxes.

Contribution to a 401(k) plan must not exceed certain limits described in the Internal Revenue Code. The limits apply to the total amount of employer contributions, employee elective deferrals and forfeitures credits to the participant's account during the year. The contribution limits apply to the aggregate of all retirement plans in which the employee participates. The contribution limits have been increased over time. Below is a chart of the contribution limits:

Year	Employee Contribution Limit	Employer Contribution Limit	Total Contribution	Catch Up Contribution (only for individuals Age 50+)
1999	$10,000	$20,000	$30,000	0
2000	$10,500	$19,500	$30,000	0
2001	$10,500	$24,500	$35,000	0
2002	$11,000	$29,000	$40,000	$1,000
2003	$12,000	$28,000	$40,000	$2,000
2004	$13,000	$28,000	$41,000	$3,000
2005	$14,000	$28,000	$42,000	$4,000
2006	$15,000	$29,000	$44,000	$5,000
2007	$15,500	$29,500	$45,000	$5,000
2008	$15,500	$30,500	$46,000	$5,000
2009	$16,500	$32,500	$49,000	$5,500
2010	$16,500	$32,500	$49,000	$5,500
2011	$16,500	$32,500	$49,000	$5,500
2012	$16,500	$33,500	$50,000	$5,500
2013	$17,000	$34,000	$51,000	$5,500
2014	$17,500	$34,500	$52,000	$5,500
2015	$18,000	$35,000	$53,000	$6,000

If an individual was aged 30 in 1999, the absolute maximum that he could have contributed including the maximum employer contributions would be $746,000.

Minimum Age Requirements

In the United States, the general minimum age limit for employment is 14. Because of this, an individual may make contributions into 401(k) plans from this age if the terms of the plan allow it. The federal government does not legally require employers to include employees in their 401(k) plans until they are at least 21 years of age. If you are at least 21 and have been working for your employer for at least one year, your employer must allow you to participate in the company's 401(k) plan. As a result, some employers' plans

will not allow individuals to invest until they are at least 18 or 21 depending upon the terms of the plan.

One-Participant 401(k) Plans

A one-participant 401(k) plan are sometimes called a solo 401(k). This plan covers a self-employed business owner, and their spouse, who has no employees. These plans have the same rules and requirements as other 401(k) plans, but the self-employed individual wears two hats, the employer and the employee.